The Forgotten I in IIoT: A Vulnerability Scanner for Industrial Internet of Things

***Rob Antrobus**[*], **Benjamin Green**[*], **Sylvain Frey**[†], **Awais Rashid**[‡]*

[*]*Lancaster University, UK ({r.antrobus1, b.green2}@lancaster.ac.uk)*
[†]*University of Southampton, UK (s.a.f.frey@soton.ac.uk; now at Google DeepMind)*
[‡]*Bristol Cyber Security Group, University of Bristol, UK (awais.rashid@bristol.ac.uk)*

Keywords: security vulnerabilities; industrial control systems; cyber-physical systems; industrial IoT; Programmable logic controllers.

Abstract

In moving towards highly connected integrated systems, the Industrial Internet of Thing (IIoT) promises a wealth of benefits. Enhanced usage of existing data sources, and integration of additional generation points, provide system users with greater visibility of industrial processes. This visibility can be used to identify and address inefficiencies. Within the context of discrete manufacturing, examples include reduction of waste materials and energy consumption. However, while one becomes engrossed in the use of big-data analytics, cloud technologies, and seamless adoption through hardware gateways, decade old systems are dropped into a technological melting pot of modern IoT, with little consideration of additional cyber security risks. Numerous works have provided evidence to suggest industrial systems are highly vulnerable to cyber attacks, from both a device and communication protocol perspective, yet efforts to automatically identify vulnerabilities are limited. This presents a significant gap, with vulnerability exploitation harbouring potentially life-threatening impact. Here we address this gap through the development of PIVoT Scan, an industrially-aware vulnerability scanner, capable of assessing a diverse range of devices and communication protocols predominantly situated within the legacy layers of IIoT environments — "The forgotten I". Furthermore, we demonstrate PIVoT Scan's ability to outperform a leading vulnerability scanner, Nessus.

1 Introduction

Over recent years we have seen a shift in technological offerings for use within Industrial Control Systems (ICSs), branded under the term Industrial Internet of Things (IIoT). These promise a wealth of benefits through seamless integration with existing systems. However, should one consider the vulnerable state of existing systems, and the critical functions they provide, the additional cyber security risks that manifest from such high connectivity may dampen this enthusiasm.

ICSs are highly complex socio-technical environments, offering monitoring, control, and automation functions across a variety of sectors. These include water, gas, oil, nuclear, etc. some of which can be considered critical national infrastructure [1]. Security challenges harboured by legacy components have been well-documented, with real-world attacks acting as an additional evidence base. Historic targets have included a uranium enrichment plant [2], energy distributions networks [3, 4], and a steel mill [5]. Legacy devices including Programmable Logic Controllers (PLCs) and Remote Terminal Units (RTUs), alongside IIoT data acquisition gateways, present an attractive attack surface. The use of legacy communication protocols, including Modbus/TCP, Ethernet/IP, DNP3, and OPC DA, further compounds the challenges, as there was little consideration for cyber security during their conception.

The integration of IIoT into traditional ICSs is blurring the boundaries as to what constitutes either system. As adoption of IIoT increases, there must be adequate consideration of security vulnerabilities that comprise the legacy layers of IIoT environments, *the forgotten I*. Figure 1 depicts a typical deployment of IIoT alongside legacy ICSs. Here we see PLCs and RTUs residing on the same local IP network as IIoT gateways, one of which is directly polling PLCs for operational data. This same gateway is then communicating with two IIoT analytic platforms via a public communication medium (i.e. the internet).

Such interaction with legacy ICS devices is often required in the deployment of IIoT. Furthermore, once data is aggregated at a local-level, its value can only be seen in its application to remote, often cloud-based, analytic platforms. In search of an affordable approach to its transit, public networks can be employed. This, alongside unrestricted interactions with legacy devices, presents a significant problem from a security perspective. However to fully realise the level of risk posed, one must be able to identify device and communication-level vulnerabilities across a wide range of legacy systems.

Currently, such vulnerability analysis is limited due to a lack of *industrially-aware* vulnerability scanners. Existing approaches and tools are based on retrofitting traditional IT vul-

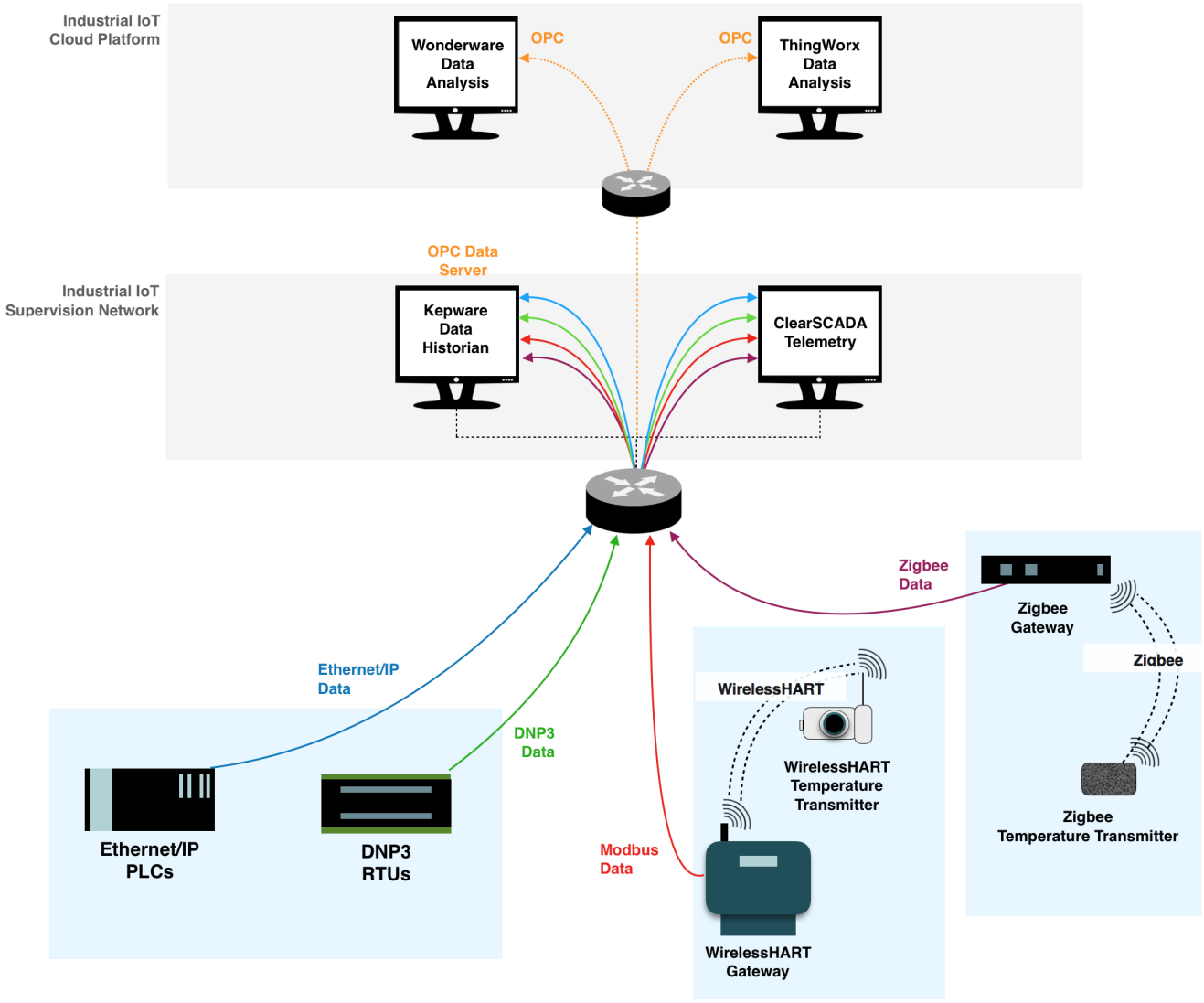

Fig. 1: A typical IIoT environment – Legacy and non-legacy devices, protocols and services

nerability scanners to an industrial context. This results in an inability to comprehensively identify vulnerabilities in legacy systems. Their effectiveness is further limited by the inherent heterogeneity of legacy components integrated within IIoT. While identification of vulnerabilities across a range of contemporary IIoT devices is important, extension towards aforementioned legacy systems, including both devices and network protocols, is critical.

In this paper we address these two fundamental challenges: the need for industrially-aware vulnerability scanners and effective support for the heterogeneous devices and protocols prevalent in IIoT. We present PIVoT Scan (Producing awareness of the Industrial-Vulnerable of Things), a vulnerability scanner tailored to the discovery of vulnerabilities in IIoT including the legacy devices integrated therein. Unlike existing scanners that simply enumerate devices, PIVoT Scan maps device information to industrial protocols, making it industrially-aware – including support for a range of heterogeneous devices and protocols. Our evaluation in a real-world IIoT testbed demonstrates PIVoT Scan's ability to outperform the leading commercial vulnerability scanner, Nessus. This is especially true when considering industrial protocols, a feature not yet present in commercial offerings. PIVoT Scan's ability to uncover vulnerabilities previously unknown to system owners and operators, offers a highly valuable tool, especially where infrastructure-wide IIoT adoption is under way.

2 Limitations of current vulnerability scanners

The market leader for commercial vulnerability scanners is Nessus. Though initially designed for scanning generic IT infrastructures, a number of plugins are available to scan for vulnerabilities in industrial devices, for example PLCs, RTUs and data acquisition gateways that are typical of IIoT environments. However, this broad approach in vulnerability scanning

impacts effectiveness, especially when deployed over a complex network consisting of a multitude of device types – something that is very much characteristic of IIoT. Prior research [6] has demonstrated that, while Nessus can uncover a number of generic IT vulnerabilities such as default credentials, insecure SSH and weak configuration of services, the coverage of specific vulnerabilities that are unique to IIoT is highly limited. Such studies demonstrate the need for industrially-aware vulnerability scanners that account for the specificities of legacy devices and protocols that make up a significant portion of IIoT environments.

A number of lightweight port scanners have been developed for IIoT protocols, including PLCScan [7] that can enumerate the Modbus/TCP and S7 protocols, the enip-info Nmap script [8] to enumerate the EtherNet/IP protocol and the dnp3-info Nmap script [9] to enumerate the DNP3 protocol. Even though these port scanners/scripts do provide pertinent information as output, e.g., firmware version number, they do not provide any information on vulnerabilities or security issues associated with a device or protocol.

In our earlier work [10], we developed the SimaticScan vulnerability scanner, specifically tailored for Siemens PLCs and the S7 protocol. However, the scanner is limited to Siemens devices only and does not address the heterogeneity of devices and protocols typical of IIoT settings.

In contrast with existing works, PIVOT Scan is:

- industrially-aware, i.e, tailored towards finding vulnerabilities in IIoT devices, including legacy ICS devices and legacy industrial protocols;
- accounts for the inherent heterogeneity of IIoT settings and supports active verification of vulnerabilities.

3 PIVoT Scan

The system architecture of PIVoT Scan is shown in Figure 2. The modular design allows users to choose which devices and protocols they want to scan, with the default option scanning all devices and protocols based on the IP addresses of devices provided as input. All modules run in parallel to each other and the modular design allows a user to select which module to run, for example, a user can scan a device for just protocol vulnerabilities. A modular architecture also makes it possible to easily integrate support for additional (new or legacy) devices and protocols as required.

The Device Enumeration and Protocol Vulnerabilities modules address the *industrial-awareness* need. The Enumeration module does not only output pertinent vulnerabilities of industrial devices but is also used as a basis to determine which CVEs to retrieve and which industrial protocols to verify. For example, should a PLC have an EtherNet/IP port open, PIVoT Scan identifies which vulnerabilities exist on the device based on its firmware version number and goes further than other vulnerability scanners in providing vulnerability information that sits outside the confines of a CVE entry, such as links to exploits and security advisories. This same kind of knowledge is then used to scan for protocol vulnerabilities, correlating the type of device and type of protocol.

The Device Vulnerabilities and Web Server Vulnerabilities modules address the *hetereogeneity* requirement – supporting vulnerability scanning for not only contemporary IIoT devices but also legacy industrial devices.

An Industrially-aware Scanner

Device enumeration. Based on the devices under test, using existing Nmap scripts, PIVoT Scan retrieves device information such as type of PLC, vendor, serial number, etc. This device information is used to determine which protocol to scan. The firmware version of a device is also retrieved and compared to vendor-specific Common Platform Enumeration (CPE) terms, a naming scheme for software, operating systems and hardware. The vFeed API [11] is used to compare the retrieved firmware version numbers with vFeed's search functionality. If the firmware of a device is less than or equal to a vendor's CPE, then it is likely that a vulnerability exists, as CVEs are correlated to CPEs. CVE information is then communicated to the user. In contrast with existing scanners, which only output relevant CVE information, PIVoT Scan is much more contextual in that it establishes information on any Metasploit modules or exploits that are available for a particular CVE, as well as any relevant security advisories from the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

Protocol vulnerabilities. IIoT supervision networks often rely on insecure legacy protocols to pull data from devices in the production network, specifically, Modbus/TCP, EtherNet/IP and DNP3. Consequently, we aim to ascertain potential protocol vulnerabilities associated with a device:

Verify Man-in-the-middle (MITM) vulnerability: A serious vulnerability that affects most industrial protocols is that of a MITM vulnerability. An attacker can leverage this to snoop on traffic and issue malicious write requests to devices that would result in false information being sent to services in the supervision network. PIVoT Scan verifies this vulnerability by attempting to ARP-spoof sessions between devices in the production network and the services that pull control process data in the supervision network. If PIVoT Scan can sniff packets between entities than this functionality is indicative of a MITM vulnerability and can also be used in verifying the presence of cleartext data.

Verify cleartext data: Another well-known vulnerability of industrial protocols is that sensitive control process data is

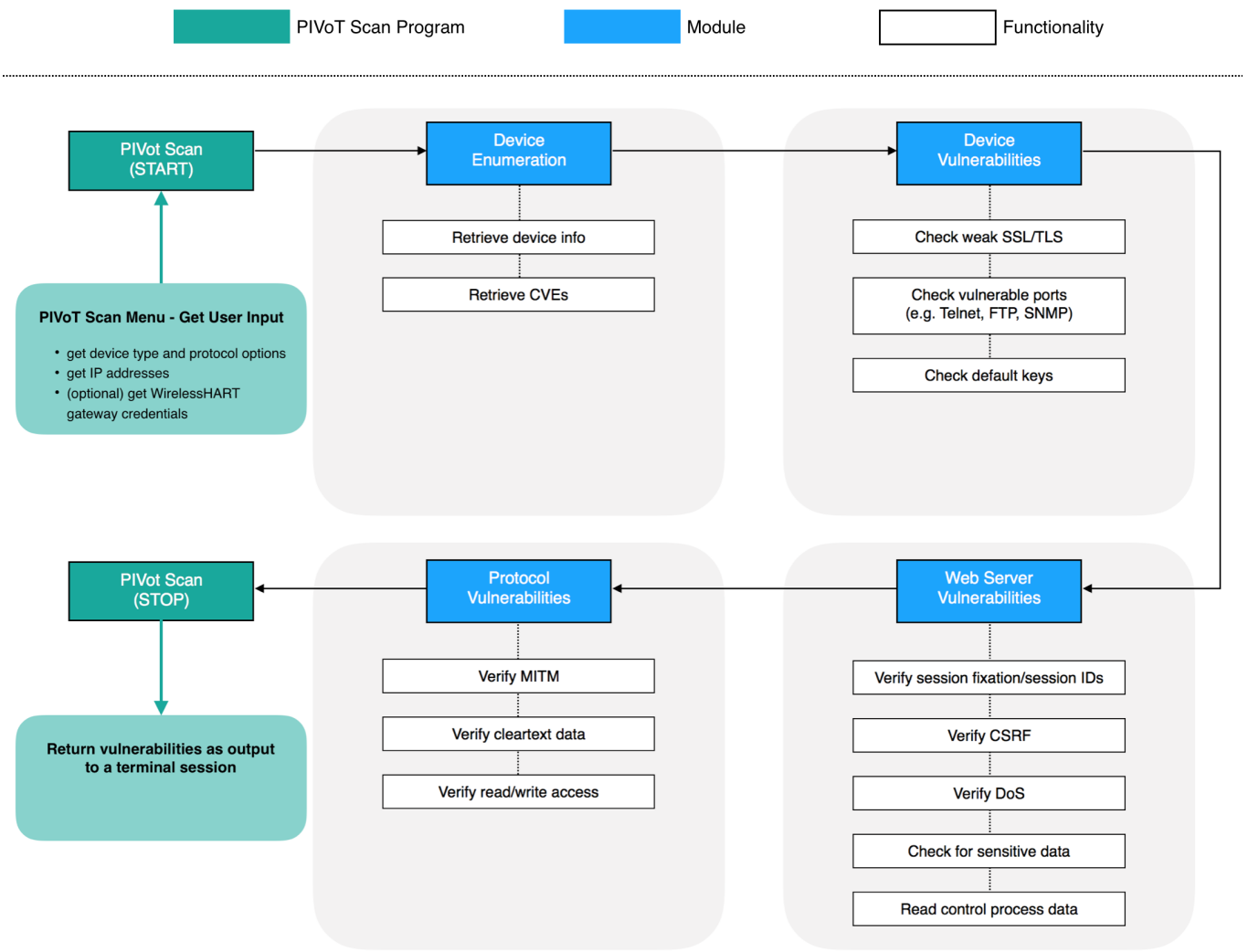

Fig. 2: PIVoT Scan System Architecture

unencrypted as it passes between devices and services. An attacker can make use of this and determine how devices operate by obtaining cleartext control process data and using this data as further basis for an attack, such as maliciously overwriting control process data. PIVoT Scan parses industrial protocol network layers at the same time as performing a MITM attack. It then traverses a protocol's application layer to identify cleartext packets.

Verify read/write access: Legacy, industrial protocols also suffer from a complete lack of authentication, which would allow attackers to issue read requests and write requests to devices/services. The *pymodbus* library for Modbus/TCP devices and the *pycomm* library for EtherNet/IP devices are used to issue read requests to devices that use these protocols. Any responses from read requests indicate that an attacker can directly read and/or write to and from legacy ICS devices and obtain data on critical control processes. Write requests are, as a conscious design choice, not supported as these have the potential to cause damage to physical control processes.

Support for Device Heterogeneity

Device vulnerabilities. PIVoT Scan supports verification of the susceptibility of a range of devices to a number of vulnerabilities. This includes scanning for:

- *vulnerabilities in the SSL/TLS* implementation, such as weak ciphers (e.g., inadequate bit length, weak protocol implementation and weak certificate signatures);
- *vulnerable ports*, probing open ports and cleartext communication or weak authentication for protocols such Telnet and FTP as well as for insecure versions of protocols such as SNMP;
- *credential scanning* for default keys, for instance, for IIoT data acquisition gateways, such as WirelessHART gateways.

Web server vulnerabilities. Several legacy ICS devices have built in web interfaces, allowing for remote monitoring and control. PIVoT Scan verifies the presence of such vulnerabilities:

Verify session fixation/session IDs: Devices that are encumbered with insecure methods of generating session IDs are tested. Attackers may conduct fixation attacks to gain access to user accounts or session hijacking attacks to gain unauthorised access to the gateway's web server. PIVoT Scan tests for this vulnerability by parsing, for instance, the URL of the WirelessHART gateway and determining if the login page has a static session ID.

Verify cross-site request forgery (CSRF): Associated with the session fixation/session ID vulnerability is the possibility of an attacker conducting a CSRF attack whereby the attacker can use the session ID to carry out malicious commands that are, in fact, carried out by a victim's browser. PIVoT Scan tests if the forms on the web server lack an unpredictable token for each user. Without a token, an attacker can forge malicious requests and is further aided in such attempts through the use of static server-generated session IDs.

Verify Denial-of-Service (DoS): This optional module offers the possibility to conduct a DoS attack on integrated web servers. Since the test could be seriously disruptive on any production system, the functionality is kept optional. When the option is enabled, PIVoT Scan performs a slowloris DoS attack to test for this vulnerability. A slowloris DoS attack is a type of DoS over the HTTP protocol, where a multitude of connections are established. These connections send long term requests which would consume a web server's connection pool. Eventually the web server will not be able to connect to other entities (i.e. an authorised user of the web server) until these held connections are released.

Check for sensitive data: Some PLCs have web servers that display sensitive control process and device information data without the need for user authentication. Any leakage of sensitive information would allow an attacker to build up a knowledge base of how a PLC works and should be kept confidential. PIVoT Scan tests for these vulnerabilities by probing the web server of a PLC and determining if it can read sensitive data such as internal PLC diagnostics.

Read control process data: Specific PLCs may have web pages open that leak sensitive control process data that should be kept confidential. An attacker can browse to this page, conduct an analysis of what the PLC is measuring and access data tags and values from this page without authenticating. PIVoT Scan determines if vulnerable web pages are open and attempts to pull data associated with control process data, such as measurements of a PLC's input and output interfaces.

4 Evaluation

We evaluated PIVoT Scan in a real-world testbed environment at Lancaster University, contrasting it with the leading vulnerability scanner, Nessus. The Lancaster testbed implements the abstract view of an IIoT environment shown earlier in Figure 1. This IIoT implementation forms part of a larger environment [12, 13]. The testbed covers a range of popular vendors and technologies, from both legacy and modern aspects of IIoT, hence offering a diverse and realistic lab-based environment.

At a device level, four Allen-Bradley PLCs, one Schneider RTU, one Siemens WirelessHART Gateway, and one Digi Zigbee Gateway, were configured for use on a local IP network. For reference, we selected four Allen-Bradley PLCs to represent a wider range and age of similar devices.

From a software perspective, Schneider's Wonderware, and PTC's Kepware and Thingworx were selected. This reflects real-world local (Kepware) and remote (Thingworx and Wonderware) data aggregation/analysis. While these are not directly included within our evaluation, they allow relevant connections to be established between our selection of devices, in the same way as if applied to a live environment.

Both PIVoT Scan and Nessus were used on the same configuration of the testbed and all identified vulnerabilities manually verified. The comparison is based on Nessus 6.10.8, the latest version of Nessus in August 2017 (when the experiments were conducted).

PIVoT Scan. As shown in Figure 3 PIVoT Scan identified a wide range of vulnerabilities across the devices/protocols in the testbed. In particular, most of the PLCs under test had relevant CVEs returned, with the ControlLogix and CompactLogix subject to 8 publicly-known vulnerabilities and 4 Metasploit modules. Almost all of the devices were running vulnerable ports, such as unencrypted Telnet and FTP ports and an insecure configuration of the SNMP protocol. Weak SSL/TLS issues were found across both IIoT gateways and one specific gateway was using default join keys.

The most serious web server vulnerabilities were found on the WirelessHART gateway, where it was subject to session fixation, CSRF and DoS vulnerabilities. The PLCs under test were leaking sensitive information from their integrated web servers and one PLC was vulnerable to a direct read of control process data via its integrated web server.

All three protocols were successfully tested. PIVOT Scan verified MITM vulnerabilities and extracted cleartext data from the Modbus/TCP-enabled WirelessHART gateway, as well as directly issuing unauthorised read requests. The same vulnerabilities were verified against the EtherNet/IP-enabled Micro 820 PLC and the SLC5/05 PLC as these were subject to unauthorised read requests. Successful spoofing of data via MITM and the attainment of cleartext data was also shown to be a vulnerability of the DNP3-enabled RTU.

PIVoT Scan Results													
Device	Device Enumeration		Device Vulnerabilities			Web Server Vulnerabilities					Protocol Vulnerabilities		
	Return device info	Retrieve CVEs	Weak SSL/ TLS	Vulnerable ports	Default keys	Session fixation/ session IDs	CSRF	DoS	Sensitive data	Read process data	MITM	Cleartext data	Unauthorised read/write access
Zigbee Gateway	—	—	✓	✓	—	—	—	—	—	—	—	—	—
WirelessHART Gateway	—	—	✓	✓	✓	✓	✓	✓	—	—	✓	✓	✓
CompactLogix PLC	✓	✓	—	✓	—	—	—	—	✓	—	—	—	—
ControlLogix PLC	✓	✓	—	✓	—	—	—	—	✓	—	—	—	—
SLC5/05 PLC	✓	✓	—	✓	—	—	—	—	✓	✓	—	—	✓
Micro820 PLC	✓	—	—	—	—	—	—	—	—	—	✓	✓	✓
Schneider RTU	—	—	—	✓	—	—	—	—	—	—	✓	✓	—

Fig. 3: PIVoT Scan results

Nessus. Figure 4 shows the results of the Nessus scans superimposed on the PIVoT Scan results in Figure 3. The red crosses indicate a vulnerability that was verified by PIVoT Scan but not by Nessus. The rightmost columns show the additional vulnerabilities that Nessus verified but PIVoT Scan did not.

The results show that Nessus did return a large number of vulnerabilities associated with device enumeration and the issues of weak SSL/TLS and vulnerable ports. It was also able to issue unauthorised read requests over Modbus/TCP to the WirelessHART gateway. The Nessus scan also additionally found an SNMP DDoS vulnerability for the ZigBee gateway, an IP forwarding vulnerability for both CompactLogix and ControlLogix PLCs and an FTP port bounce vulnerability for the Schneider RTU.

Comparing PIVoT Scan and Nessus results. Though both PIVoT Scan and Nessus were able to return device information for the PLCs, Nessus was unable to retrieve any CVEs associated with the PLCs. While both scanners were adept at finding SSL/TLS vulnerabilities and unsecured ports, the default join key vulnerability, a specific IIoT vulnerability, was not verified by Nessus.

Nessus was unable to determine the vulnerabilities of the WirelessHART gateway's web server and was only capable of determining that HTTP services were running. Similarly, with the PLCs, Nessus did not infer that the information on the PLC's web server was of a sensitive nature. In contrast PIVoT Scan could not only verify the aforementioned vulnerabilities but also directly read control process data from a table that was residing in the SLC5/05's web server.

PIVoT Scan was a lot more effective in determining the vulnerabilities of industrial protocols than Nessus. For instance, although Nessus was able to check for unauthorised read/write access over the Modbus/TCP protocol, it could only read data from two locations associated with the device, whereas PIVoT Scan was able to read data from four locations. The Modbus/TCP protocol was also tested by PIVoT Scan for a MITM vulnerability, which verified that the protocol was communicating in cleartext and could be easily spoofed. For the EtherNet/IP protocol, PIVoT Scan was able to verify both MITM and cleartext data vulnerabilities for the Micro820 PLC, as well as directly verifying the unauthorised read/write access vulnerability. In contrast, Nessus incorrectly identified read vulnerability of Modbus/TCP data from the Micro820 PLC, which was manually verified to be not the case. For the DNP3 protocol, again Nessus was not able to determine a MITM vulnerability and/or the issue of having control process data as cleartext from the Schneider RTU and was unable to determine that the DNP3 protocol was running at all.

However, the Nessus scan did return vulnerabilities that PIVoT Scan did not. A SNMP reflection DDoS vulnerability was verified that would give attackers the ability to conduct a reflective DDoS attack over the Zigbee gateway. Two of the PLCs were liable to IP forwarding vulnerabilities where an attacker

Nessus Scan Results																
Device	Device Enumeration		Device Vulnerabilities			Web Server Vulnerabilities					Protocol Vulnerabilities			Nessus-specific Vulnerabilities		
	Return device info	Retrieve CVEs	Weak SSL/TLS	Vulnerable ports	Default keys	Session fixation/ session IDs	CSRF	DoS	Sensitive data	Read process data	MITM	Cleartext data	Unauthorised read/write access	SNMP DDoS	IP Forwarding Enabled	FTP port bounce
Zigbee Gateway	—	—	✓	✓	—	—	—	—	—	—	—	—	—	✓	—	—
WirelessHART Gateway	—	—	✓	—	✗	✗	✗	✗	—	—	✗	✗	✓	—	—	—
CompactLogix PLC	✓	✗	—	✓	—	—	—	—	✗	—	—	—	—	—	✓	—
ControlLogix PLC	✓	✗	—	✓	—	—	—	—	✗	—	—	—	—	—	✓	—
SLC5/05 PLC	✓	✗	—	✓	—	—	—	—	✗	✗	—	—	✗	—	—	—
Micro820 PLC	✓	—	—	—	—	—	—	—	—	—	✗	✗	✓ (false positive)	—	—	—
Schneider RTU	—	—	—	✓	—	—	—	—	—	—	✗	✗	—	—	—	✓

Fig. 4: Nessus scan results

can route packets through the host and the Schneider RTU was liable to an FTP port bounce vulnerability, where attackers could use the remote server to connect to third parties using the PORT command.

5 Conclusion

The wide range of vulnerabilities that PIVoT Scan successfully evaluated shows how the complexity and heterogeneity of IIoT environments leads to security vulnerabilities. The use of insecure, legacy protocols will remain an issue for some time. However, asset owners and control systems engineers can tailor defensive measures for these protocols based on industrially-aware vulnerability scanning tools.

Our comparison of PIVoT Scan and Nessus demonstrates the importance and effectiveness of such industrially-aware scanners, especially with respect to legacy devices and protocols integrated into IIoT enviroments. Although much work has been done on contemporary devices and protocols, the legacy issue of IIoT still requires scrutiny and practical tools such as PIVoT Scan can help in uncovering vulnerabilities and driving innovation in developing defensive tools and frameworks.

Acknowledgements.

This work is supported by the EPSRC Research Hub on Cyber Security of Internet of Things (PETRAS) project IoTinControl (EP/N023234/1) and the EPSRC/CHIST-ERA grant DYPOSIT: Dynamic Policies for Shared Cyber-Physical Infrastructures under Attack (EP/N021657/1; EP/N021657/2).

References

[1] B. Green, M. Krotofil, and D. Hutchison, "Achieving ICS Resilience and Security Through Granular Data Flow Management," in *Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy*. ACM, 2016, pp. 93–101.

[2] D. Kushner, "The real story of Stuxnet," *IEEE Spectrum*, vol. 50, no. 3, pp. 48–53, 2013.

[3] Dragos, "Crash Override: Analysis of the Threat to Electrical Grid Operations," https://dragos.com/blog/crashoverride/CrashOverride-01.pdf, 2017, [Accessed 06 February 2017].

[4] T. Pultarova, "News Briefing: Cyber security-Ukraine grid hack is wake-up call for network operators," *Engineering & Technology*, vol. 11, no. 1, pp. 12–13, 2016.

[5] R. M. Lee, M. J. Assante, and T. Conway, "German Steel Mill Cyber Attack," SANS, Tech. Rep., 2014. [Online]. Available: https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks{_}Facility.pdf

[6] S. Samtani, S. Yu, H. Zhu, M. Patton, and H. Chen, "Identifying SCADA vulnerabilities using passive and active vulnerability assessment techniques," in *Intelligence and Security Informatics (ISI), 2016 IEEE Conference on*. IEEE, 2016, pp. 25–30.

[7] S. Hilt, "Scanning PLC Devices – PLCScan," http://www.digitalbond.com/blog/2013/05/14/scanning-plc-devices-plcscan/, 2013, [Last Accessed 02 February 2017].

[8] Nmap, "enip-info," https://nmap.org/nsedoc/scripts/enip-info.html, 2016, [Accessed 15 January 2017].

[9] S. Hilt, "Nmap-NSEs/dnp3-info.nse," https://github.com/sjhilt/Nmap-NSEs/blob/master/dnp3-info.nse, 2015, [Accessed 16 February 2017].

[10] R. Antrobus, A. Rashid, S. Frey, and B. Green, "SimaticScan: Towards a specialised vulnerability scanner for industrial control systems," *4th International Symposium for ICS & SCADA Cyber Security Research*, 2016.

[11] vFeed, "Trusted Vulnerability & Threat Intelligence Database," https://www.owasp.org/index.php/Testing_for_Weak_SSL/TLS_Ciphers,_Insufficient_Transport_Layer_Protection_(OTG-CRYPST-001), 2017, [Last Accessed 02 February 2017].

[12] B. Green, D. Hutchison, S. A. F. Frey, and A. Rashid, "Testbed Diversity as a Fundamental Principle for Effective ICS Security Research," in *Proceedings of International Workshop on Security and Resilience of Cyber-Physical Infrastructures (SERECIN), held in conjunction with International Symposium on Secure Software and Systems (ESSoS)*, 2016.

[13] B. Green, A. Lee, R. Antrobus, U. Roedig, D. Hutchison, and A. Rashid, "Pains, Gains and PLCs: Ten Lessons from Building an Industrial Control Systems Testbed for Security Research," in *10th USENIX Workshop on Cyber Security Experimentation and Test (CSET 17)*. USENIX Association, 2017.